PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/167

A1

(11) International Publication Number: **WO 98/43430**

(43) International Publication Date: 1 October 1998 (01.10.98)

(21) International Application Number: PCT/EP97/02106

(22) International Filing Date: 25 April 1997 (25.04.97)

(30) Priority Data:
97400650.4 21 March 1997 (21.03.97) EP
(34) Countries for which the regional or international application was filed: FR et al.

(71) Applicant *(for all designated States except US)*: CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André Citroën, F-75711 Paris Cedex 15 (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: FICHET, Laurent [FR/FR]; 20, rue des Francs Compagnons, F-78320 Le Mesnil Saint Denis (FR). DE LA TULLAYE, Pierre [FR/FR]; 7, allée Marcel Jouhandeau, F-92500 Rueil Malmaison (FR). DE SARZENS, Philip [FR/FR]; 24, rue de Saint Quentin, F-75010 Paris (FR). JEZEQUEL, Jean-François [FR/FR]; 35, rue du Commandant Kieffer, F-95240 Cormeille en Parises (FR).

(74) Agent: COZENS, Paul, Dennis; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).

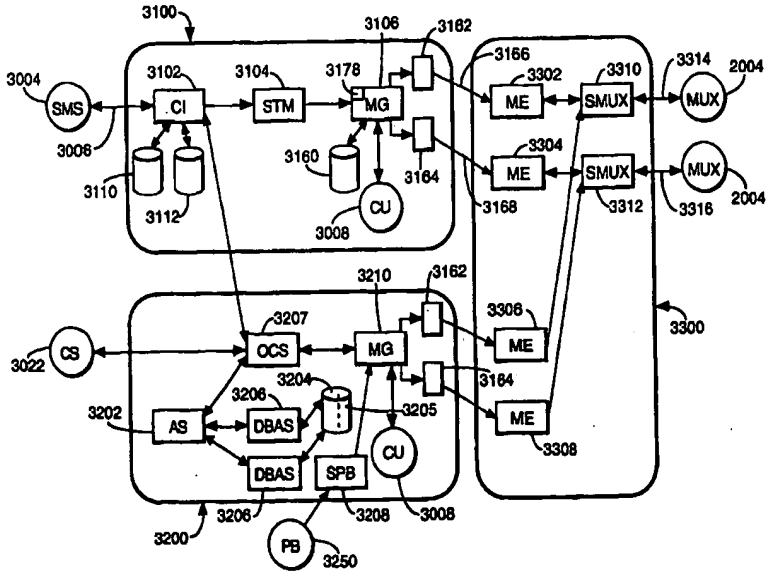
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SIGNAL GENERATION AND BROADCASTING

(57) Abstract

The invention includes a mostly conventional digital television system (2000) to transmit compressed digital signals. A multiplexer (2004) receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter (2008) of the broadcast centre via linkage (2010). The transmitter (2008) transmits electromagnetic signals via uplink (2012) towards a satellite transponder (2014), where they are electronically processed and broadcast via notional downlink (2016) to earth receiver (2018). The signals received by receiver (2018) are transmitted to an integrated receiver/decoder (2020) connected to the end user's television set (2022). The receiver/decoder (2020) decodes the compressed MPEG-2 signal into a television signal for the television set (2022). A conditional access system (3000) is connected to the multiplexer (2004) and the receiver/decoder (2020), and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to one or several television programmes sold by the broadcast supplier, can be inserted into the receiver/decoder (2020). Using the decoder (2020) and smartcard, the end user may purchase commercial offers in either a subscription mode or a pay-per-view mode. A number of features of particular interest are disclosed, involving the randomization of EMMs, mixing parameter length and identifier on EMMs and the like to save space, dynamic allocation of bandwidth for specific EMMs, and the STM being separate from the SMS.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

SIGNAL GENERATION AND BROADCASTING

The present invention relates to a broadcast system, to a conditional access system for the broadcast system, to a broadcast and reception system, to apparatus for generating signals (including messages), to analogous methods, and to signals for use with the aforesaid systems, apparatus and methods.

In particular, but not exclusively, the invention relates to a mass-market broadcast system having some or all of the following preferred features:-

- It is an information broadcast system, preferably a radio and/or television broadcast system
- It is a satellite system (although it could be applicable to cable or terrestrial transmission)
- It is a digital system, preferably using the MPEG, more preferably the MPEG-2, compression system for data/signal transmission
- It affords the possibility of interactivity.

Again, in particular but not exclusively, the invention relates to a Subscriber Authorization System (SAS) forming part of a conditional access system for a broadcast system. By an SAS is preferably meant any device, apparatus or system for authorizing users to have access to the conditional access system, regardless of the end use. The SAS might be for use with a radio and/or television broadcast system, but equally could be for authorizing users, for example, in computer networks, in parking lots, and so on. The SAS preferably also has the function of generating suitable entitlement messages.

A function of known Subscriber Authorization Systems is to manage access rights to television programmes, available as commercial offers and sold according to different modes of commercialisation (subscription mode, pre-book mode, impulse mode). The SAS, according to those rights and to information received from a Subscriber Management System (SMS), generates using a message generator so-called "Entitlement Management Messages" (EMMs) which are broadcast by a message

emitter via a multiplexer to a receiver/decoder of the subscriber to authorize him/her.

In a known system, the message emitter has no ability to sense or control what it emits to the multiplexer. Hence it has been realized pursuant to the present invention that it is possible that the message emitter may transmit back to back two EMMs which are to be received and decoded by the receiver/decoder. In such circumstances, it is possible that if the EMMs are insufficiently separated the receiver/decoder will be unable to sense and decode properly the second of the EMMs. This may create severe authorization problems.

The present invention in a first aspect seeks to solve this and other problems.

According to a first aspect of the present invention, there is provided apparatus for repetitively generating a set of messages, comprising:

means for generating a plurality of messages;

means for repetitively randomizing the sequence of the messages to form a plurality of sets of such messages, so that the messages of each set are in random sequence; and

means for outputting the plurality of sets of messages.

By repetitively randomizing the sequence of the messages the chance of two messages being broadcast only back to back after a number of repetitions can be made negligibly small.

Preferably, the message generating means includes means for storing the generated messages, and, if so, the randomizing means is preferably arranged to form each said set of messages by retrieving the messages in random sequence from the storage means. This can be a particularly efficient way of putting the invention into practice, since the messages do not then have to be generated again each time the sequence of the messages is randomized.

For ease of access, the storage means is preferably arranged to store the messages in

an at least two-dimensional array. Further dimensions may be added, for example to represent the different operators for whom the messages may be generated.

Preferably, the apparatus further comprises means coupled to the output means for varying the rate at which the plurality of sets of messages is output. In this way any bitrate directive from the multiplexer can be taken account of.

For the same reason, the apparatus preferably further comprises means coupled to the storage means for evaluating the size of the messages stored in the storage means, and means coupled to the output means for varying the rate at which the plurality of sets of messages is output, in dependence upon the said size of the messages.

Preferably, the generating means and the randomizing means are coupled via a First In First Out device. Since these two components may be a large distance apart, provision of the FIFO device can allow them effectively to run independently in case of failure of one of them. For the same reason, the output means preferably includes means for storing at least one of the sets of messages, so that, again, it can effectively operate in standalone mode.

A plurality of output means may be provided, in which case the apparatus preferably further comprises a multiplexer for receiving the plurality of sets of messages output by said plurality of output means.

The present invention extends to an access control system for a broadcast and reception system, said access control system including, at the broadcast end, apparatus as aforesaid, and, at the reception end, a device for receiving said messages.

The message may be an entitlement message for broadcast to the receiving device. In turn, the entitlement message may be an EMM or ECM. In the preferred embodiment, the output means comprises an EMM Injector for injecting EMMs into the stream of data to be broadcast.

The present invention further extends to a broadcast and reception system including an access control system as aforesaid; the system may be for the digital broadcast of television programmes.

The present invention also extends to a method of repetitively generating a set of messages, comprising:

generating a plurality of messages;

repetitively randomizing the sequence of the messages to form a plurality of sets of such messages, so that the messages of each set are in random sequence; and

outputting the plurality of sets of messages.

Preferably, the method includes the step of storing messages generated in the generating step, and in the randomizing step preferably each said set of messages is formed by retrieving the messages in random sequence.

The invention also provides a method of controlling access of a user to a broadcast and reception system, including, at the broadcast end, a method of repetitively generating a set of messages as aforesaid, and, at the reception end, the step of receiving said messages. Preferably, the message is an entitlement message for reception by the receiving step.

A further aspect of the present invention is now discussed. Conventionally in the broadcast of a digital bitstream, information is transmitted as a packet of digital data and an identifier for the packet; the identifier is at least two bytes in length.

According to the present invention, preferably the output means referred to before is arranged to output the plurality of sets of messages as a digital signal including a packet (more preferably several packets) of digital data and an identifier for the packet, the identifier being less than two bytes (and preferably one byte or less) in length. This can result in a reduced bandwidth requirement.

The feature is provided independently. Hence, according to a second aspect of the

present invention, there is provided apparatus for generating a digital signal comprising a packet of digital data and an identifier for the packet, comprising:

means for generating the packet of data; and

means for generating the identifier;

wherein:

the identifier generating means is arranged to generate an identifier which is less than two bytes in length.

The identifier may comprise an identity parameter and a length parameter, in which case preferably these parameters are each 4 bits in length for ease of implementation.

Preferably, the digital value of the length parameter is not directly proportional to the actual length of the packet. This can permit a greater range of actual length of the packet than the range of the digital value of the length parameter. The apparatus may further comprise means for storing a look-up table giving the correspondence between the digital value of the length parameter and the actual length of the packet.

This aspect of the present invention also extends to a broadcast and reception system including, at the broadcast end, apparatus as aforesaid, and, at the reception end, a device for receiving said signal.

Furthermore, in the method as aforesaid the plurality of messages may be output as a digital signal comprising a packet of digital data and an identifier for the packet, the identifier being less than two bytes in length.

In its independent method form, the second aspect of the present invention provides a method of generating a digital signal comprising a packet of digital data and an identifier for the packet, comprising:

generating the packet of data; and

generating the identifier;

wherein:

the identifier is less than two bytes in length.

Preferably, the identifier comprises an identity parameter and a length parameter. Preferably also, the digital value of the length parameter is not directly proportional to the actual length of the packet.

The second aspect of the present invention also provides a digital signal, comprising:

a packet of digital data; and

an identifier for the packet;

wherein:

the identifier is less than two bytes in length.

Preferably, the identifier comprises an identity parameter and a length parameter, the identity and length parameters are each 4 bits in length, and the digital value of the length parameter is not directly proportional to the actual length of the packet.

A third aspect of the present invention is now discussed. Conventional broadcast systems are typically subject to severe bandwidth restraints.

Therefore, preferably, if the broadcast and reception system as aforesaid further comprises means for broadcasting data, it also comprises means for producing a control command representative of a characteristic of the data, and the output means includes means for repetitively broadcasting the plurality of sets of messages, at a variable repetition rate, and for varying the repetition rate in response to the control command.

This feature is, in the third aspect of the present invention, provided independently. According to this third aspect, there is provided a broadcast system, comprising:

means for broadcasting data;

means for producing a control command representative of a characteristic of the data; and

means for repetitively broadcasting a message, at a variable repetition rate; said message broadcasting means being arranged to vary the repetition rate in response to the control command.

By varying the repetition rate in response to the control command, bandwidth can be allocated dynamically for specific messages.

In the preferred embodiment, the data are signals representative of programme events (preferably digital television or radio programme events), and the means for producing the control command is arranged to produce the command to be representative of the time of broadcast of a particular programme event, and preferably further the message is an EMM. This aspect of the invention is particularly relevant to Pay Per View events, where the demand by viewers for authorization to watch a particular PPV event will generally vary according to the proximity of the event.

The control command may be produced by the programme broadcaster, possibly through a so-called "Server for Programme Broadcaster" (SPB).

Preferably, said message broadcasting means is arranged to vary the repetition rate near the time of broadcast of the event. Preferably also, said message broadcasting means is arranged to increase the repetition rate before the time of broadcast of the event, as well as to increase the repetition rate during the time of broadcast of the event.

For example, for a particular PPV programme event the increased rate may start perhaps 30, 20, 15, 10 or 5 minutes before the time of broadcast of the event, and may continue until perhaps one half of, three-quarters of or even the entirety of the event has elapsed. The lower rate may be one broadcast every 30 or 15 minutes, whilst the increased rate may be one broadcast every 2 or one minutes or every 30 seconds. The actual rate naturally does not have to be exactly the figures mentioned; intermediate figures are also possible, and the lower rate may be slower than once every 30 minutes and the increased rate may be faster than once every 30 seconds.

The third aspect of the invention extends to a broadcast and reception system including, at the broadcast end, a system as aforesaid, and, at the reception end, a device for receiving the broadcast data and messages.